***** PUBLIC VERSION *****

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

UNITED STATES OF AMERICA, Plaintiff, v. ZACKARY ELLIS SANDERS, Defendant.	Case No. 1:20-cr-00143 Honorable T.S. Ellis, III Trial: October 19, 2021 HEARING REQUESTED

MEMORANDUM IN SUPPORT OF MR. ZACKARY ELLIS SANDERS'S RENEWED MOTION TO SUPPRESS BASED ON LACK OF PROBABLE CAUSE AND FALSE AND MISLEADING STATEMENTS AND FOR A *FRANKS* HEARING

Zackary Ellis Sanders, by and through undersigned counsel, and pursuant to Federal Rule of Criminal Procedure 41 and the Fourth Amendment, respectfully renews his motion to suppress all evidence obtained pursuant to the invalid search warrant issued in this case because it was not supported by probable cause and was based on an affidavit containing numerous false and misleading statements.[1]

It is necessary for Mr. Sanders to renew and supplement his earlier motions to suppress evidence for two reasons. First, the defense is indisputably correct that the Foreign Law Enforcement Agency's ("FLA's") tip, which the Federal Bureau of Investigation ("FBI")

[1] This motion renews and supplements Mr. Sanders's Motion to Suppress Due to Lack of Probable Cause (Motion to Suppress No. 1) (Dkt. 81-82), Motion to Suppress Based on False and Misleading Material Information in Affidavit Paragraph 23 (Motion to Suppress No. 2) (Dkt. 85-86), and Motion to Suppress Based on Materially Misleading Statements and Omissions Regarding Tor, the Target Website, and the Subject Premises (Motion to Suppress No. 3) (Dkt. 83-84). Mr. Sanders also incorporates by reference the following prior pleadings and related exhibits: Dkt. 93, 109, 112, 137, 140, 176, 241, 335, and 426.

understood to mean that an IP address associated with the Sanders family's home was used on a single occasion to visit a website that included links to, *inter alia*, child pornography, was insufficient to establish probable cause. The Court's prior ruling reflects a clear error of law justifying reconsideration.

Second, the record supporting Mr. Sanders's motions is significantly stronger and more well developed than it was when Mr. Sanders filed his original motions to suppress. This is primarily the result of the government's untimely compliance with its discovery obligations, including under Federal Rule of Criminal Procedure 16 and *Brady v. Maryland*, 373 U.S. 83 (1963), with respect to screenshots of the [redacted] website, as well as other factual developments demonstrating that the government has been misleading the Court in this case regarding the FBI's contemporaneous understanding of the FLA's tip. The new evidence warranting reconsideration includes: (1) the four exculpatory screenshots the government produced months late in violation of its *Brady* obligations; (2) the Criminal Complaint (Dkt. 354-9) from [redacted] in which the government's representations to the Court in this case were contradicted by the FBI itself; (3) other material from the defense's investigation into this case (which the government has actively sought to impede). Neither the additional screenshots nor the [redacted] Complaint were available to Mr. Sanders when he originally filed his motions to suppress and are accordingly newly discovered evidence warranting reconsideration. Mr. Sanders's renewal of his suppression motion provides the Court with the opportunity to rule on a more complete record and, in the event the matter proceeds to an appeal, will allow the Fourth Circuit to do the same.

INTRODUCTION

This case presents a straightforward legal question under the Fourth Amendment: does a tip from a Foreign Law Enforcement Agency ("FLA") that an Internet user on a single occasion visited an unknown part of an onion service website that within the site contains links to, *inter alia*, child pornography, without more (such as evidence that the user registered for the site or viewed any illegal content), supply probable cause for a search warrant? The answer is clearly no. Both the facts here and the governing law fully support that conclusion.

The Court has reasoned to the contrary based on a factually discredited version of the FLA's tip and, more substantively, on a misconception regarding the number of "affirmative steps" an Internet user must undertake in order to visit the website at issue here (the nature of which the government and in turn the Court have repeatedly mischaracterized). The Court's affirmative steps theory of probable cause is not viable. As the declarations of qualified experts Seth Schoen, Dr. Steven Murdoch, Dr. Richard Clayton, and Dr. Matthew Miller make abundantly clear—as well as demonstrative videos from Mr. Schoen that are attached as Exhibit 1 (A and B)—navigating to an onion service website is easily accomplished and in fact requires very few "affirmative steps." In fact, once a user has downloaded the Tor Browser (one needs a browser to visit any website), the process for visiting an onion service website like the target website is not different from visiting a website on the open Internet. And no court has ever found that a single visit to a regular Internet site that contains child pornography—without more—supplies probable cause; the cases support precisely the opposite proposition.[2] The fact that the content available through [redacted] to a registered, logged-in user is not exclusively child pornography makes that legal conclusion all the more unavoidable. Because the Court's

[2] *See* Memorandum in Support of Motion to Suppress No. 1 (Dkt. 82) at 10-11 (compiling cases).

prior ruling on Mr. Sanders's motions to suppress were predicated on incorrect facts and a "clear error of law," *Zinkand v. Brown*, 478 F.3d 634, 637 (4th Cir. 2007), the Court should reconsider its prior ruling and suppress all evidence obtained as a result of the government's illegal warrant.

BACKGROUND

The Court is familiar with much of the factual background. In order to have it all in one place, however, Mr. Sanders repeats certain of that background here as well as recounts the evidence that is newly discovered since he filed his motions to suppress on September 2, 2020.

A. Tor is easy to both download and use, including with respect to onion service websites.

1. Downloading the Tor Browser

The Tor Browser is a software application that people use to access the Tor network and thereby browse websites on both the open Internet (what people usually think of when they think of the Internet) and onion services websites.[3] *See, e.g.*, Miller Decl. (Dkt. 254-4) at ¶ 7 ("The Tor Browser is a browser that uses the Tor Network to connect to the Internet. It has the ability to browse 'open' Internet websites as well as Tor Onion Service websites"); Schoen Decl. (Dkt. 256-7) at ¶¶ 7-20 (explaining that the Tor Browser was developed by the 501(c)(3) non-profit called the Tor Project to protect users' privacy, and that the US government is one of its main sponsors).

[3] "Onion service websites" are websites that are only accessible via Tor. Miller Decl. 1 (Dkt. 254-5) at ¶ 7. They were previously referred to as hidden services, but the Tor Project, the 501(c)(3) organization that created the Tor Browser, now refers to them as onion services. Law enforcement sometimes refer to onion services as "hidden services" or "dark web" sites. *Id.*

When the [redacted] website operated (before it was seized in June 2019), Internet users could visit it, other onion service websites, or open Internet websites by using the Tor Browser.[4]

It is simple to download the Tor Browser—even for someone who is not technically sophisticated. Video: How to Download Browsers (Ex. 1-A); Schoen Decl. (Dkt. 256-7) at ¶¶ 32-38; Clayton Decl. (Dkt. 256-8) at ¶ 36 ("Using TOR is extremely easy – one downloads the 'TOR bundle' for Windows, Mac or for one's phone or tablet. One then installs it and launches it and it can immediately be used. On a fast connection this takes less than a minute."). For example, a person can go to the Tor Project website, at https://www.torproject.org/download/, and with one or two clicks[5] download the Tor Browser for free. Downloading the Tor Browser from the Tor Project website takes no more than a couple minutes. Video: How to Use Browsers (Ex. 1-B);

[4] Mr. Sanders has elsewhere discussed the many legitimate reasons for people to use Tor. *See, e.g.,* Schoen Decl. (Dkt. 256-7) at ¶¶ 21-31 (people may be drawn to Tor Browser over other browsers, including Google Chrome, Apple Safari, Microsoft Edge, or FireFox, because of the features, including those that protect users' IP addresses, that "can help reduce what people reveal about themselves and prevent several different forms of online tracking," including avoiding companies' profiling people's interests, helping people avoid targeted ads, helping people avoid location tracking, helping people avoid geoblocking, helping people avoid Internet censorship, allowing people to research topics without revealing where they work, and allowing people to send anonymous tips to journalists and law enforcement); *see also* Notice of Supplemental Authority (Dkt. 112) (explaining how Department of Justice anti-trust case against Google demonstrates why people have good reasons for downloading and using the Tor Browser as their browser of choice, including to avoid being "forced to accept Google's policies, privacy practices, and use of personal data," which the government itself criticized as being less privacy-protective for consumers).

[5] Some browsers (and depending on how people have configured their browsers) will ask a person to confirm that they want to download a file, while others will start downloading immediately after a person clicks the download button.

Schoen Decl. (Dkt. 256-7) at ¶¶ 39-41 (describing the steps required to download the Tor Browser and providing screenshots to provide a visual explanation).

Downloading the Tor Browser is precisely the same as downloading any Internet browser, such as Mozilla Firefox or Google Chrome. *Id.* at ¶ 36; Video: How to Download Browsers (Ex. 1-A); Miller Fourth Decl. (Dkt. 253-7) at ¶ 11 ("The Tor Browser is an easy to use program that can be easily installed just like any other browser, like Firefox, Chrome, or Opera.").[6] The Tor Browser was specifically designed to be easy to use, so that the public could have free, easy-to-access, heightened security protections online. Schoen Decl. (Dkt. 256-7) at ¶¶ 35-37; *see* Clayton Decl. at ¶ 36. Once a person has downloaded the Tor Browser, to browse the Internet they simply need to open the program by clicking on its icon—just like they would for any other browser. Schoen Decl. (Dkt. 256-7) at ¶ 42; Video: How to Use Browsers (Ex. 1-B).

2. Using the Tor Browser is simple.

Once a person has opened the Tor Browser, it operates in substantially the same way as any other web browser. *See Id.* at ¶¶ 42-43 (providing a screenshot of the Tor Browser). There is a web address bar where a person can enter the address of the website they want to visit. *Id.* at 7 (screenshots provide a visual explanation). There is also a default search engine bar where a person can enter search terms. *Id.* at 8. For example, if a person used the default search engine bar, they could search for "eastern district of virginia u.s. district court" and the search engine would display the results. *See id.* at 8 (providing a screenshot of search results on the Tor Browser). A person could then use the Tor Browser to visit this Court's website. *See id.* at 9

[6] If someone wanted to download Google Chrome or Mozilla Firefox, they would simply need to search for terms such as "web browsers" or "Google Chrome" or "Mozilla Firefox" specifically in a search engine and then follow the same steps as described by Mr. Schoen required to download the Tor Browser, *i.e.* they would simply visit the relevant download page and download the software. Video: How to Download Browsers (Ex. 1-B); Schoen Decl. (Dkt. 256-7) at ¶¶ 39-41.

(providing screenshot of the "Court's website as visited with the current version of Tor Browser" and noting "[t]he process of navigating to it, and the site's appearance, were much the same as in any other web browser").

There are also a number of search engines for onion service websites, which Internet users can locate simply by searching, for example, "Tor search engine." Video: How to Use Browsers (Ex. 1-B). Conducting such a search using the "Tor Browser address bar (as of June 2021) will offer 5 different search engines for Tor Onion Services." Murdoch Decl., attached as Ex. 2, at ¶ 46. As a result, "[t]here is no need to use an index to find a Tor Onion Service because search engines are easily available from Tor Browser with just a few clicks." *Id.* at 46; *see also* Schoen Decl. (Dkt. 256-7) at 12 (providing a screenshot of search results using a search engine called "Torch" on the Tor Browser); *see also* Ex. B to Murdoch Decl. (Ex. 2) (providing screenshots of search results for "BDSM"). Because there are fewer onion service websites than there are websites on the open Internet, "it is easier for a user to visit all sites returned for a search." Murdoch Decl. (Ex. 2) at ¶ 47.

3. Connecting to an onion service website is easily accomplished and does not require special knowledge of the site's alpha-numeric URL address, or even an intent to visit a particular site.

As with elsewhere on the Internet, someone on Tor need not know the exact URL address of a website in order to visit it, but would more easily and more commonly use a search engine. *Id.* at ¶¶ 45-47. One could also easily click a hyperlink or visit a website that contains part of another website. *See* Schoen Decl. (Dkt. 256-7) at ¶¶ 62-63 (explaining how people can easily click on links without knowing where they will lead); *see also* Murdoch Decl. (Ex. 2) at ¶¶ 56-58 (explaining that "[i]t is common that a single website will contain parts of other websites" and why "someone may include part of one Onion Service website within another"). While

"Paragraph 27 of the search warrant implies that searching to discover the address of an onion service website is difficult and requires the use of a directory site," that is incorrect because of the ease with which one can use search engines on Tor. Murdoch Decl. (Ex. 2) at ¶¶ 45-47.[7] Someone can visit a website by clicking on a search engine result without necessarily knowing what it will contain, because results can be different than people expect and because search engines are almost never able to show password-protected content in the description of the site. Schoen Decl. (Dkt. 256-7) at ¶¶ 48-56. In addition, people can also click on hyperlinks without knowing where they will lead. *Id.* at ¶¶ 57-77.

Because people can easily click on search results or hyperlinks without understanding where they will lead, a visit to a website does not necessarily imply that a person intended to view particular content or visit a particular website. Indeed, there is actually an incentive for people to try to attract people to visit their websites who may not have otherwise intended to go there, because "some Onion Services are supported by advertising, just as with the open Internet," and "Onion Services who wish to protect the privacy of their operator and users visiting them may wish to increase the traffic to the website;" consequently, "[s]earch results may be intentionally misleading to attract more users who might not necessarily be interested in the content the website contains." Murdoch Decl. (Ex. 2) at ¶ 49. This incentive may be particularly strong for websites that may contain contraband, and they may even embed part of their website in another non-contraband website to, for example, "inflate the number of visitors

[7] It is important to note that "Paragraph 27 of the search warrant affidavit also implies that directories of Onion Service addresses give accurate and clear indications of whether these services contain unlawful material. This is not necessarily the case. Some directories are open to editing by anyone and are not moderated. A person who wishes to promote an Onion Service may list the address while not indicating that the content is unlawful. . . [T]his could be because, for example, the person wants to attract more users who are not motivated by illegal content but may nevertheless visit." Murdoch Decl. (Ex. 2) at ¶¶ 50-51.

to the website, to create cover traffic, [or] to advertise content." *Id.* at ¶¶ 56-58. Thus, "[j]ust because someone visits a website, it does not imply that they intended to visit that website or view content on that website." *Id.* at ¶ 55.

B. The investigation into an onion service website called "[redacted]

Since at least as far back as January 2019, the FBI was investigating an onion service website called [redacted][8] Any photos, videos, and links on [redacted] were password-protected. None of the pages available to a user who was not registered or logged in displayed pornography, much less child pornography, or any image at all. *See, e.g.,* Homepage (Dkt. 176-1), Announcements Page (Dkt. 176-4), Registration Page (Dkt. 354-1) at 3, and Login Page (Dkt. 354-1 at 4). An Internet user could only view illegal content on [redacted] after registering an account, logging in, and taking additional affirmative steps to click on and open postings with illegal content within specific topics or forums. *Id.* at ¶ 24 (stating that Internet users "were required to create an

[8] It appears U.S. law enforcement actually began investigating [redacted] sometime prior to 2017, when a joint operation between the U.S. Department of Homeland Security and [redacted] law enforcement led to the arrest and conviction of an administrator. [redacted] Given the length of time the U.S. has been investigating this site, and the fact that the FBI was investigating this and other sites "in conjunction" with the [redacted] the FBI would have understood the meaning of the FLA's tip. *See, e.g.,* Affidavit in Support of Criminal Complaint and Arrest Warrant (Dkt. 4) at ¶ 9 ("The FBI, in conjunction with other law enforcement entities, is investigating websites on which visitors can access and view child sexual abuse material. Through this investigation, the FBI received information that on or about May 23, 2019, an individual connected to the internet through a specific [IP] address and accessed a website.").

account (username and password) in order to access the majority of the material"). Thus, to view illegal content on [redacted] (or any other photos or videos), an Internet user had to (1) go past [redacted] homepage; (2) register an account; (3) login using his account credentials; (4) navigate to a forum; (5) select a sub-forum; and (6) search for and click on a forum post that opened illegal content. *See* Board Index and Screenshots (Dkt. 256-10) at 1-2 (screenshot of page only visible to a user who had gone past the homepage, registered an account, and logged in, which shows that further affirmative steps were required for someone to actually then view illegal content).

[redacted] appears to have used "phpBB forum software," which is "one of the most popular tools for creating Internet discussion forums." Schoen Decl. (Dkt. 256-7) at ¶ 78. In such forums, Internet users "don't see the images that have been posted in a forum topic unless they click on that individual topic." *Id.* at ¶ 80. With phpBB forums, Internet users "typically have to click on several links in order to view a specific forum topic or post." *Id.* Thus, "[o]n a phpBB forum like [redacted] creating an account and logging in can enable users to see and interact with password-protected portions of the forum . . . but after registering an account and logging in, users would still have to take affirmative steps to view specific content," whether that content was legal or illegal. *Id.* at ¶ 83. Furthermore, "[b]ased on the screenshot of the target website's homepage, the site's homepage did not indicate the nature of the content available to logged-in users. Therefore, the target website may [have] appear[ed] in searches for innocuous keywords," such as a search for "BDSM" or wrestling. Murdoch Decl. (Ex. 2) at ¶ 48, Ex. B.

C. The government's selective disclosure of the FBI's [redacted] screenshots

The FBI captured numerous screenshots of [redacted] in January 2019, six months before a foreign law enforcement agency seized the website in June 2019. Affidavit at ¶ 15. Because [redacted] was shut down, these screenshots constitute the only evidence the government has

produced of how [redacted] appeared to a visitor to the website and, in the case of a person who registered and logged in, a user. Over the course of 2020 and 2021, the government disclosed a total of eight "screenshots" originally taken by the FBI in January 2019. The first four screenshots were produced to the defense on July 27, 2020. Screenshot of Post Described in Paragraph 16 Taken by FBI in January 2019 (Dkt. 256-9); Additional Screenshots Taken by FBI in January 2019 (Dkt. 256-10). Three of these screenshots (Dkt. 256-10) show content on [redacted] that an Internet user could click on only after registering an account and logging in, which the Internet user at issue here was not alleged to have done. There is no allegation that the Internet user in this case ever viewed any of the pages depicted in the screenshots the government disclosed in July 2020 (Dkt 256-9, Dkt. 256-10).

In December 2020 and January 2021, the government produced four additional screenshots—screenshots (Dkt. 174-1, 174-4, and 354-1 at 3-4) the defense had been asking for since the outset of this case and, indeed, had unsuccessfully moved to compel as *Brady* and Rule 16 material. Even though the government was in possession of these screenshots, it did not disclose them until several months *after* the Court had resolved Mr. Sanders's original motions to suppress on October 26, 2020.

The withheld screenshots depict pages that an Internet user *would have to visit* before being able to view or download any illegal content at all, and conclusively show that there is a difference

between a user accessing just any page of [redacted] and accessing child pornography.[9] This evidence accordingly increases the likelihood that a person who visited [redacted] just one time did not intend to—and did not—view anything illegal (or attempt to). The four additional screenshots also underscore the fact that [redacted] did not "advertis[e]" child pornography and that not every page was "dedicated" to child pornography. *But see* Affidavit (Dkt. 254-3) at ¶ 15 (Agent Ford claiming that [redacted] was "dedicated to the advertisement and distribution of child pornography"). The screenshots establish that there is no pornography of any kind on the publicly available pages (or any images suggestive of such) and reinforce that one could not view or download "online child sexual abuse and exploitation material" on [redacted] without logging in with a username and password.[10] These screenshots therefore contradict Agent Ford's description of the website to the Magistrate.

D. The [redacted] Communications to the FBI in 2019

In the second half of 2019, the FBI received communications from the [redacted] that the government characterizes as a "tip." According to the government, there are three documents

[9] While there is no evidence of specific content that the Internet user in this case allegedly accessed, the [redacted] definition of child sexual abuse and exploitation material, also known as [redacted]

[10] The government has never provided an explanation for its untimely compliance with its discovery obligations nor has the Court noted the government's violation of its discovery duties. The Court's approach to an allegedly untimely filing by the defense has not been equally generous. *See, e.g.*, 09/08/21 Order (Dkt. 457).

comprising the purported tip: the Intel Log (Dkt. 253-1), the [redacted] Letter (Dkt. 253-2), and the Intelligence Report (Dkt. 253-3). According to the government, the FBI received these three single-page communications from the [redacted] respectively, on August 19, September 16, and October 25, 2019. According to the government, these three single-page documents "make up the entire substance of the tip that we were provided." July 31 Hearing Transcript (Dkt. 253-13) at 25; *see also id.* at 26 (explaining to the Court that the three single-page [redacted] Intelligence reports are "the extent of the tip"). As set forth below, the defense contests this assertion, given the ample evidence—including Agent Ford's own statements from his affidavit—demonstrating that the government continues to withhold additional discovery.

C. The government continues to withhold documents relevant to the [redacted] tip.

Taking the three purported tip documents together, it is clear that these are *not* the only documents relevant to the [redacted] tip. The Affidavit supporting the search warrant itself, *see infra* at 29, states that the FLA in August 2019 "named and described . . . the TARGET WEBSITE," Affidavit at ¶ 23, and that the FLA "provided further documentation naming the website as the TARGET WEBSITE, which the FLA referred to by its actual name," *id*. at ¶ 24. And yet, the government has never produced—and the Court has repeatedly declined to compel it to produce—that document. In fact, the government has never produced any document linking Mr. Sanders's IP address to the website [redacted] The only "tip" document the government has produced mentioning [redacted] is the October 25, 2019 Intelligence Report (Dkt. 253-3), which has a different operation name from the Intel Log ("[redacted] vs. "[redacted] and—as the government concedes—has nothing directly to do with Mr. Sanders's case, but was merely provided to the defense as "contextual information," Gov't Opp'n (Dkt. 43) at 5—whatever that may mean. As the FBI was aware, there were a variety of sites, in addition to [redacted] that the

FBI and the [redacted] were investigating, so there is no clear basis for assuming that the FLA intended to communicate that the Internet user had visited [redacted] as opposed to a different target site. Affidavit in Support of Criminal Complaint and Arrest Warrant (Dkt. 4) at ¶ 9 (Agent Obie noting that the FBI and FLA were investigating, "in conjunction with" one another, numerous sites); Affidavit (Dkt. 254-3) at ¶ 26 (Agent Ford noting that tips provided by the FLA related to numerous sites).

Furthermore, the Affidavit submitted in support of the search warrant indicates that the target website was *not* [redacted] The computer server hosting the target website was seized by a foreign law enforcement agency in June of 2019. Affidavit at ¶ 15. Nonetheless, Agent Ford averred to the Magistrate in February 2020 that the target website had "active users." Affidavit at 9 n.1 ("The name of the TARGET WEBSITE is known to law enforcement. Investigation into the users of the website remains ongoing and disclosure of the name of the website *would potentially alert active website users to the investigation*." (emphasis added)). Both things cannot be true: either the website was seized in June 2019 and no longer had users, or it was not seized and was still operating in February 2020, when Agent Ford submitted his affidavit. Absent a reckless disregard for the facts (requiring a *Franks* hearing on that ground, as well), the only explanation for Agent Ford's statement that the target website had active users in February 2020 is that the "target website" the Internet user allegedly visited was not, in fact, [redacted]

D. The FBI understood the [redacted] tip to mean the specified IP address was used to visit the target website one time.

It is indisputably clear that, at the time Agent Ford submitted his Affidavit to Magistrate Anderson, the FBI understood the correct meaning of the FLA's tip: that the Internet user had visited an unknown part of a target website on one occasion. FD-1057 (Dkt. 253-4) at 2. The FBI further understood that although accessing content on the target website required login credentials

(a username and password), the [redacted] was not claiming to have any evidence of this Internet user having acquired or employed those credentials. The Court's ruling that there is "no evidence—either in documents generated by the [FLA] or by the FBI—that Special Agent Ford thought [the FLA's tip meant that] defendant merely visited [redacted] homepage and did not view child sexual abuse and exploitation material," 08/21/20 Sealed Mem. Op. (Dkt. 73) at 10, is simply wrong and a "clear error of law" warranting reconsideration. *Zinkand*, 478 F.3d at 637.

That the FBI understood that the Intel Log (Dkt. 253-1) was communicating only that the Internet user visited a website is abundantly clear from:

- Agent Ford's own, internal FBI case opening memo, (Dkt. 253-4), from January 17, 2020 (less than three weeks before he submitted the Affidavit), in which his description of the Internet user's actions as conveyed by the FLA is limited to "access[ing] [redacted] on a single date, at a single time.[11] *Id.* at 2. Agent Ford did not mention the Internet user accessing child pornography or "child sexual abuse and exploitation material," as he would have done had he believed such evidence to exist.

- The February 10, 2020 search warrant affidavit itself, which at least *six times* characterizes the Internet user's activity as merely "accessing" [redacted] and only one time—when paraphrasing and embellishing the FLA's tip in paragraph 23—suggests that the Internet user "accessed child sexual abuse and exploitation material via a website." *See* Affidavit (Dkt. 254-3) at ¶ 6 ("There is probable cause to believe that a user . . . accessed the TARGET WEBSITE."); *id.* at 15 (heading describing "Evidence Related to Identification of the Target that Accessed the TARGET WEBSITE"); *id.* at ¶ 26 ("tips provided by the FLA regarding IP addresses that the FLA advised were associated with access to child-exploitation-related web and chat sites"); *id.* at ¶ 29 (explaining that "accessing the TARGET WEBSITE required numerous affirmative steps"); *id.* at ¶ 30 ("[T]here is probable cause to believe that any user who accessed the TARGET website has . . . knowingly accessed the TARGET WEBSITE with intent to view child pornography, or attempted to do so."); *id.* at ¶ 31 ("the IP address 98.169.118.39, which the FLA reported was used to access TARGET WEBSITE on May 23, 2019"); *see also id.* at ¶ 24 (using the exact same language the Intel Log had used to describe the "material" the Internet user purportedly accessed to describe the website as a whole). Thus, at least six times in the Affidavit, the Agent set forth his understanding of the limits of the FLA's tip as accessing a website, and not viewing child pornography.

[11] Again, the defense does not know why Agent Ford stated that the target website was [redacted] in his report, given that the defense has been provided with no document linking Mr. Sanders's IP address to the [redacted] website.

- Agent Obie's March 19, 2020 statements in the affidavit submitted in support of the Criminal Complaint (Dkt. 4) in this case, which again characterized Mr. Sanders's activity as having "*accessed* a website" and reflected an understanding that the investigation of this and other websites had been conducted by the FBI "in conjunction" with the FLA. *Id.* at ¶ 9 (emphasis added).

- The government's April 1, 2020 representation to the Court in support of Mr. Sanders's pretrial detention that Mr. Sanders merely "*accessed a website* that advertises child pornography." Gov't Opp'n at 2 (Dkt. 15) (emphasis added).

- The [redacted] 2021 criminal complaint from *United States v.* [redacted], which *accurately* describes the FLA's tip as meaning that, [redacted] (emphasis added).

On the government's side, the evidence supporting the position that Agent Ford believed the FLA had evidence of the Internet user actually viewing or attempting to view illegal content (as opposed to just visiting the website) is nil. Other than the Intel Log's ambiguous language, the government has yet to produce a single other document suggesting in any way that Special Agent Ford or any other individual at the FBI actually believed that the FLA had evidence of Mr. Sanders viewing or attempting to view illegal content on [redacted] or any other website. *See* September 11 Hearing Transcript (Dkt. 137-1) at 25 ("MR. CLAYMAN: . . . Admittedly, we don't know precisely what the content is, but we have never claimed to know exactly what it is, or exactly the definition of child pornography under the United States Code. We also never claimed that the tip alleges that he downloaded that content.").

In contrast to the abundant evidence supporting the defense's position, there is simply nothing to support the government's view of the tip other than an incorrect reading of the Intel Log's ambiguous language, which is only possible when that language is read in isolation from everything else. The government has spilled much ink attacking the plain logic of the defense's

interpretation of the tip—which relies on the FBI's own words—but it has not offered a single document to support its argument that Agent Ford believed the FLA's tip to mean it had evidence of the Internet user accessing or attempting to access illegal content, despite submitting an additional affidavit from Agent Ford himself. Ford Affidavit (Dkt. 254-12). Agent Ford did not address his subjective understanding of the tip in that Affidavit. *Id.*

E. The Court's Opinions and Orders denying Mr. Sanders's motions.

A review of the Court's numerous Orders in this case demonstrates that the Court has simply adopted the government's arguments—even when they have contradicted one another—without regard for the actual state of the evidence.[12] The Court's Orders reflect two related but distinct errors on issues fundamental to the Fourth Amendment analysis: (1) whether Agent Ford materially altered the FLA's tip by adding the language "via a website;" and (2) whether the tip was describing the act of merely visiting the website or viewing illegal content once there.

1. Agent Ford materially altered the FLA's tip.

First, the Court has steadfastly refused to acknowledge that Agent Ford did not quote the tip verbatim but instead, as discussed, added the language "via a website." *See, e.g.,* 08/21/20 Sealed Mem. Op. and Order (Dkt. 73) at 9 (stating that "Paragraph 23 conveys the same information contained in the FLA's tip"); 10/26/2020 Sealed Memorandum Op. (Dkt. 113) at 6 (stating that "Special Agent Ford's Affidavit accurately reiterates the FLA's Tip"); *id.* at 9 ("Paragraph 23 accurately reports the FLA Tip"); *id.* at 12 (Paragraph 23 "simply repeats,

[12] The Opinions and Orders issued by the Court relevant to this motion are: 08/21/20 Sealed Mem. Op. and Order (Dkt. 73) (denying motion to compel); 09/10/20 Sealed Order (Dkt. 107) (denying motion for reconsideration); 10/26/20 Sealed Mem. Op. and Order (Dkt. 113) (denying Mr. Sanders's motions to suppress); 01/26/21 Sealed Order (Dkt. 236) (denying motion to compel), 05/26/21 Order (denying motion to compel) (Dkt. 369), 08/25/21 Order (denying motion to compel) (Dkt. 442).

essentially verbatim, the tip" and "accurately and clearly conveys the FLA tip"). The reality, however, is that Agent Ford altered the tip in a critical respect by adding the language "via a website." This addition obscured from the Magistrate the real meaning of the FLA's tip by further concealing what the FBI knew to be true, that the phrase "online child sexual abuse and exploitation material" in the Intel Log *was already referring to a website generally*. Agent Ford therefore knew that it made no sense to say that the Internet user "access[ed]" a website "via a website." Affidavit (Dkt. 254-3) at ¶ 23. By adding "via a website," Agent Ford knew that the Magistrate would believe that the Internet user had actually viewed or attempted to view specific illegal content on a website, as opposed to merely visiting the website itself. Agent Ford knew that a truthful recitation of the tip would have stated merely that the Internet user accessed a website, not what Paragraph 23 communicated (that the Internet user accessed illegal material via a website).

Indeed, Agent Ford's addition of "via a website" doubtlessly contributed to this Court being misled by Paragraph 23 of the Affidavit in the same way the Magistrate would have been, *i.e.*, believing that the FLA was describing an Internet user's specific activity on a website, as opposed to merely going to a website, notwithstanding the evidence to the contrary (which includes other sections of the Affidavit itself). In its August 21, 2020 Opinion denying Mr. Sanders's motion to compel, the Court held as follows:

> Seeking to avoid [the] result [that Paragraph 23 accurately conveys the tip's substance], defendant argues that 'via a website' appears nowhere in the FLA's tip. This argument is unpersuasive; stating that material was accessed 'via a website' adds no information *because it is obvious that the FLA's original tip describes an internet user's activity on a website*. . . . This is so because an internet user cannot access child sexual abuse and exploitation material without accessing a website that advertises and distributes child pornography.

Mem. Op. (Dkt. 73) at 10-11 (emphasis added). The Court's interpretation of the tip was precisely what the FBI led the Magistrate to believe; the problem is that it was not what the FLA intended to convey, which the FBI well knew.

Indeed, as set forth below, the Court itself later acknowledged the possibility that the "obvious" conclusion the Court had reached in its opinion denying Mr. Sanders's motions to compel was incorrect, and that the tip meant only that the Internet user accessed the website. *See* Order (Dkt. 236).

2. The Court's initial interpretation of the tip as connoting the viewing of illegal content was wrong—a possibility the Court has now recognized.

Relatedly, the Court has repeatedly assumed—without any evidence from the government on this point except the Intel Log itself; without the government ever having stated Agent Ford's understanding of the FLA's tip (despite submitting an affidavit from Agent Ford himself); and notwithstanding significant evidence to the contrary—that the FBI understood the tip to be describing specific activity on a website. *See* 8/21/20 Mem. Op. (Dkt. 73) at 11 ("There is no evidence—either in documents generated by the FLA or by the FBI—that Special Agent Ford thought defendant merely visited [redacted] homepage and did not view child sexual abuse and exploitation material."); 9/10/20 Sealed Order (Dkt. 107) at 5 ("The idea that Special Agent Ford knew that the language was misleading was pure speculation."). That is plainly incorrect. To take just one example, Agent Ford's *own internal report* states that the FBI had in August 2019 "received information from a foreign law enforcement agency (FLA) . . . that [the] FLA *identified a user who accessed* [redacted] using IP address 98.169.118.39, on May 23, 2019, at 02:06:48 UTC." FD-1057 (Dkt. 253-4) at 2 (emphasis added). The notion that Special Agent Ford believed Mr. Sanders had *accessed illegal content* and yet chose to describe that conduct in his own internal

FBI report as merely *accessing the website* defies both logic and common sense. It is accordingly the Court's order denying Mr. Sanders's motions to suppress that relies on a misreading of the tip in conjunction with the record.

Third, the Court also repeatedly states that there is no evidence—either in documents generated by the FLA or the FBI—that "Special Agent Ford thought defendant merely visited [redacted] homepage and did not view child sexual abuse and exploitation material." Mem. Op. (Dkt. 73) at 11. Given Agent's Ford's own internal report, other sections of his own Affidavit, and contradictory statements made by both the FBI and the government in this case, *supra* at 16-18, the Court's statement is obviously incorrect. The fact that the Court has chosen simply to ignore the abundant evidence supporting the Agent's understanding that Mr. Sanders only accessed the site does not make such evidence cease to exist.

Indeed, in the course of litigating Mr. Sanders's Fourth Amendment claims, the Court has articulated an alternative theory in support of probable cause which conforms to the FBI's contemporaneous understanding of the FLA's tip. In its October 26, 2020 Sealed Memorandum Opinion (Dkt. 113) denying Mr. Sanders's motions to suppress, the Court noted that "the fact that the FLA informed the FBI that defendant's IP address accessed the Tor hidden service [redacted] clearly invites and warrants the reasonable inference that the IP address user was purposeful in his efforts to reach the [redacted] website and its illegal content." *Id.* at 13. Similarly, on January 26, 2021, in denying Mr. Sanders's motion to compel, the Court offered up an alternative theory of probable cause:

> [O]n its face, the FLA Tip states that the user of the target IP address "accessed online child sexual abuse and exploitation material," not that the user accessed only the Target Website's homepage. However, even if the FLA tip were read to mean that the target IP address user visited only the Target Website's homepage, "the information in the Affidavit noting the steps the Target IP address user was required to take to navigate to the [Target Website] warrants the inference that the Target IP

> Address user's arrival at the [Target Website] was purposeful, that is the Target IP User's purpose was to access the website and its illegal content." *United States v. Sanders*, Case No. 1:20-cr-143 (E.D. Va, October 26, 2020) (Memorandum Opinion) [(Dkt. 113)].

Order (Dkt. 236) at 2, n.1. As discussed above, the Court previously assumed that the user had gone beyond the homepage and looked at illegal content, just as the Magistrate would have, as well.

ARGUMENT

I. EVIDENCE CONCEALED BY THE GOVERNMENT AND RECENTLY DISCOVERED BY MR. SANDERS WARRANTS RECONSIDERATION OF THE COURT'S DENIAL OF MR. SANDERS'S MOTIONS TO SUPPRESS.

As discussed above, the Court denied Mr. Sanders's motions to suppress on October 26, 2020 (Dkt. 113). Since that time, however, Mr. Sanders has obtained significant new evidence bearing on the violation of his Fourth Amendment rights, including exculpatory evidence that the government concealed from the Court and the defense until December 2020 and January 2021, in violation of its duties under *Brady v. Maryland*. Based on this new evidence, as well as the Court's clear error of law in upholding the warrant based on the legally and factually incorrect "affirmative steps" theory, reconsideration is appropriate here, "to account for new evidence" or to "correct a clear error of law or prevent manifest injustice." *Zinkand*, 478 F.3d at 637.

II. THE WARRANT WAS NOT SUPPORTED BY PROBABLE CAUSE.

Given the abundant evidence of what the FLA's tip actually meant—and the complete lack of any evidence supporting the government's view—it cannot be reasonably disputed at this juncture what the FLA was communicating: that an Internet user with a specified IP address went to an unknown part of a "target website" on May 23, 2019. Contrary to the Court's prior ruling, evidence of a single visit to a website—even a Tor onion service such as the target website—is not sufficient for probable cause.

Probable cause for a search warrant exists when, "given all the circumstances set forth in the affidavit . . . there is a fair probability that contraband or evidence of a crime will be found in a particular place." *Illinois v. Gates*, 462 U.S. 213, 238 (1983). A Magistrate is required to "make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him, including the 'veracity' and 'basis of knowledge' of persons supplying hearsay information, there is a fair probability that contraband or evidence of a crime will be found in a particular place." *Gates*, 462 U.S. at 238. When a reviewing court examines the validity of a search warrant, such validity "must be assessed on the basis of the information that the officers disclosed, or had a duty to discover and to disclose, to the issuing Magistrate," and not on what was uncovered afterwards during the execution of the warrant. *Maryland v. Garrison*, 480 U.S. 79, 85 (1987).

A. There was not probable cause to believe that the Internet user had committed an offense as the "affirmative steps" theory of probable cause fails under both the facts and the law.

In contrast to the misleading nature of Paragraph 23, Paragraph 29 of the Affidavit correctly states the theory of probable cause under which the FBI was requesting a warrant—which does not include the viewing or downloading of illegal content. Paragraph 29 states that "because accessing the TARGET WEBSITE required numerous affirmative steps by a user—including downloading Tor software, accessing the Tor network, finding the web address for the TARGET WEBSITE, and then connecting to the TARGET WEBSITE via Tor—it is extremely unlikely that any user could simply stumble upon the TARGET WEBSITE without understanding its purpose and content." Affidavit (Dkt. 254-4) at ¶ 29. Paragraph 30 similarly summarizes Agent Ford's case for probable cause when he avers that, based on the affirmative steps needed to reach the target website, "there is probable cause to believe that any user who accessed the TARGET

WEBSITE has, at a minimum, knowingly accessed the TARGET WEBSITE with intent to view child pornography, or attempted to do so." *Id.* at ¶ 30.

The Court's ruling that the Internet user's one-time visit to the website is sufficient for probable cause is a clear error of both law and fact that should be reconsidered. The Court's ruling is based on the factual premise that accessing an onion service website is somehow difficult or takes an unusual number of steps. That is incorrect. As this video from defense expert Seth Schoen demonstrates, Video: How to Use Browsers (Ex. 1-B), it is remarkably simple to visit an onion service website and takes no more steps than visiting a site anywhere else on the Internet.

B. Given the simplicity of accessing an onion service website, the affirmative steps theory fails as a matter of law.

Visiting a website one time—even an onion service—has never been enough for probable cause. This is because of the common-sense proposition that "[s]omeone who visits a web site only once is more likely to have found the content of that site was either not what they expected or not what they were looking for, compared to someone who visits a web site repeatedly." Schoen Decl. (Dkt. 256-7) at 10. The steps required to download and use the Tor Browser are no more complicated or suspicious than those required to download and use Google Chrome, Firefox, or any number of other browsers that most Americans use. *See* Videos (Ex. 1-A and 1-B). An Internet user does not need to type in the 16-or-56-character web address of an onion service website to find it,[13] just as one does not need to do so on the open Internet. Instead, a user can readily and easily use one of several available Tor search engines or click on a hyperlink, both of

[13] The target website's address was only "16 characters, followed by '.onion,' according to the homepage screenshot (which revealed that the address had only 16 characters before the '.onion,' not 56)." Murdoch Decl. (Ex. 2) at ¶ 6. This is not something that Agent Ford disclosed to the Magistrate, and it was not something the defense could have uncovered until after receiving the screenshot of the homepage (Dkt. 174-1), which it did only in December 2020.

which can easily lead an Internet user somewhere they were not expecting or intending. *See e.g.,* Murdoch Decl. (Ex. 2) at ¶¶ 45-58; Schoen Decl. (Dkt. 256-7) at ¶¶ 48-77.

The caselaw fully supports this proposition. *See, e.g., United States v. Falso*, 544 F.3d 110, 120-21 (2d Cir. 2008) (finding no probable cause when all that was alleged was that defendant "*appear[ed]" to have "gained access* or *attempted to gain access*" to a website with a name suggestive of child pornography, which contained 11 images of child pornography and which advertised additional child pornography at an internet address that was hidden until a membership was purchased *and there was no allegation that he subscribed* to the paying-membership site); *cf. United States v. Goodwin*, 854 F.2d 33 (4th Cir. 1988) (finding probable cause for anticipatory search warrant when defendant *ordered child pornography and investigation verified that materials would be delivered to address where warrant was executed*) (emphasis added); *United States v. Shields*, No. 4:CR-01-0384, 2004 WL 832937, at *7 (M.D. Pa. Apr. 14, 2004), *aff'd*, 458 F.3d 269 (3d Cir. 2006) (finding probable cause where it was clear that defendant *voluntarily subscribed to and joined two websites* whose purpose was to share child pornography); *United States v. Froman,* 355 F.3d 882, 890–91 (5th Cir. 2004) (finding probable cause where defendant *paid to join a group* called Candyman where the sole purpose was to receive and distribute child pornography, defendant *registered screennames that reflected an interest in child pornography*, and defendant *did not cancel his paid subscription* to the group) (emphases added).

In its October 26, 2020 Sealed Memorandum Opinion (Dkt. 113), the Court relied on *United States v. Bosyk,* 933 F.3d at 319, in support of the "affirmative steps" theory. *Bosyk* compels precisely the opposite conclusion. In *Bosyk*, the facts were much more incriminating—and did far more to establish probable cause—than those present here. The affidavit in *Bosyk*: "(1) identifie[d] the existence of a[n] [onion service] website, [Bulletin Board A,] which cater[ed]

specifically to a community of users looking to trade child pornography; (2) identifie[d] a *specific post* in a *sub-forum* catering to pre-teen hardcore content, which on its face provide[d] *thumbnails of child pornography* and a link to *download child pornography*; and (3) provide[d] information demonstrating that a computer with an IP address that c[ould] be traced back to the defendant's residence attempted to download the child pornography on the same day it was posted on the website." Dkt. 109-1 at 4 (emphasis added).[14] The incriminating evidence—that someone at Mr. Bosyk's residence actually clicked on the download link to download child pornography—was uncovered by the FBI itself with actual proof, as opposed to uncorroborated hearsay from a tip.

In *Bosyk*, the government asserted that "probable cause . . . was based on the fact that someone in the defendant's residence *downloaded or attempted to download* child pornography from a link located in a post at Bulletin Board A." *Id.* at 10. According to the affidavit, that post was in a specific sub-forum, entitled "Pre-teen Hardcore, sub forum Videos," and the post stated that the link contained four explicit videos. *Id.* at 6. "[B]elow the posts [we]re twenty video thumbnail images that depict[ed] an adult male using his fingers to spread the vagina of a female who appears to be a toddler." *Id.* at 6. In order "to download this content via a link provided in the post, a user had to enter a password, which was provided in the body of the post." *Id.* at 6. Anyone who visited that link could download *only* content that was illegal, and none that was legal. Thus, it was reasonable to infer that anyone who visited the website, chose the specific sub-forum, chose the specific post within it, observed thumbnail images of content that was

[14] In defending the warrant in *Bosyk*, the government stated that because "there was no reason for the agent to believe the link was available anywhere other than on Bulletin Board A" and "defendant's IP address attempted to download the file in question *the same day* the link was posted on Bulletin Board A," "[i]t is unlikely the URL was accessed somewhere else [other than the Onion Service website Bulletin Board A] given the close proximity in time between the posting at Bulletin Board A and attempt to download its child pornographic content." *Id.* at 8-9 (emphasis in original).

unambiguously child pornography, and then still clicked on the URL that unambiguously led to specific videos of child pornography, both intended and attempted to download child pornography.

In Mr. Sanders's case, the government admitted at the hearing on September 11, 2020 (Dkt. 137-1), that there was nothing specific regarding this Internet user's activity on the website, *i.e.*, no specific information about what content this Internet user purportedly accessed; no information that what this Internet user actually viewed was illegal; and no allegation that this Internet user downloaded or attempted to download child pornography. By contrast, the government admitted in *Boysk* that merely joining an e-group where child pornography was shared—which the Internet user in this case is not even alleged to have done—"falls short" of probable cause without any evidence that the person actually tried to or did possess child pornography. Dkt. 109-1 at 11-12. The government reasoned that "[w]hile merely joining an e-group without evidence that an individual either attempted to or did acquire illicit material falls short of the Fourth Amendment's requirements"—because "merely joining an e-group is not illegal"—"a click of a URL, that was advertising child pornography on a website dedicated to child pornography,[15] does establish probable cause." *Id.* at 11-12. In *Bosyk*, the "single click of a button allowed the defendant to download *four* [specific] images of child pornography." *Id.* at 12 (emphasis in original).

In upholding the warrant in *Bosyk*, the Court reasoned that "the *posting* of that *particular section* [of the website] . . . was *clearly advertising video clips of what would absolutely be unequivocally child pornography*," and "the same day that posting went up, . . . the IP address that

[15] As discussed *supra*, [redacted] was not exclusively dedicated to child pornography. The posts that described the content an Internet user could view on the website were identified as separate postings in password-protected sub-forums, not postings on the homepage of the website, and the forum topics of different categories of material were only available after an Internet user registered an account and logged in, which this Internet user is not alleged to have done.

is linked to a computer in the defendant's home . . . attempts to [initiate a download of the four videos of child pornography]." Transcript of *Boysk* Motions Hearing, attached as Ex. 2 to Gov't Opp'n (Dkt. 101-2) at 3-4 (emphases added).[16] Here, there is no evidence of the Internet user's actual activity on the website.

A single visit on a single date to a website that contained a mix of legal and illegal content cannot be enough to link a person, as the affiant claimed, to "an online community of individuals who regularly send and receive child pornography," Affidavit (Dkt. 254-3) at ¶ 6, or reasonably to infer that a person intended or attempted to view child pornography. Instead, a single visit to the website suggests the opposite: if the Internet user is alleged to have visited the website just one time, even assuming, *arguendo*, that the Internet user did inadvertently or unintentionally view child pornography, the fact that the Internet user is not alleged to have ever returned to the website suggests that child pornography was not what the Internet user was intending to view.

The Affidavit provides no basis for inferring that this particular Internet user had any intent to view or download child pornography. The Affidavit did not allege that the Internet user viewed or downloaded any specific images. *Cf. Bosyk*, 933 F.3d at 322 (in affidavit, FBI alleged defendant clicked on link contained in post with numerous thumbnail images depicting man sexually molesting female toddler), *cert. denied*, 140 S. Ct. 1124 (2020). There was no evidence that the Internet user ever kept, maintained, or used directory sites that advertised the web addresses of hidden services that contained child-exploitation-related content. Affidavit (Dkt. 254-3) at ¶ 27.

[16] The Court also reasoned that "[i]t's very unusual to see people who . . . *do look* at child pornography to not hold it for extensive periods of time." *Id.* at 4. Here, unlike in *Bosyk*, without evidence that an Internet user actually viewed or downloaded illegal content, there is nothing to connect this Internet user to a community of people with an interest in viewing and collecting child pornography. That is particularly true when the name of the website in this case was not suggestive of child pornography and the website has legal content on it.

The Affidavit did not allege that the Internet user was a website administrator or content moderator of the website. Affidavit (Dkt. 254-3) at ¶¶ 18-19. The Affidavit did not allege that the Internet user actually displayed or possessed any of the characteristics common to individuals with a sexual interest in children or visual depictions in children, as described of other users more generally in the Affidavit in paragraphs 38-44. *Id.* at ¶¶ 38-44. The Affidavit did not allege that the Internet user ever posted to the site or sent a message on the site. *Id.* at ¶¶ 17, 18.

C. The Good Faith Exception Does Not Apply.

The good faith exception to the exclusionary rule does not apply here. *See United States v. Leon*, 468 U.S. 897 (1984). The Fourth Circuit has held:

> The *Leon* good-faith exception is not available where . . . the magistrate fails to perform a "neutral and detached" function and instead merely rubber stamps the warrant [or] . . . the affidavit does not provide the magistrate with a substantial basis for determining the existence of probable cause.

United States v. Gary, 528 F.3d 324, 329 (4th Cir. 2008).

Even assuming *arguendo* that the Agent did not knowingly or recklessly mislead the Magistrate, *see supra*, the Magistrate failed to perform its neutral and detached function because the Magistrate merely rubber-stamped the bare conclusions of the FBI, who misrepresented the nature of the uncorroborated hearsay of the FLA. Furthermore, the Affidavit did not provide a substantial basis for probable cause**.** This Court has held that "a magistrate may rely on law enforcement officers, who may draw on their own experience and specialized training to make inferences from and deductions about the cumulative information available to them that might well elude an untrained person, *as long as the affidavit contains facts to support the law enforcement officer's conclusions*." *United States v. Matish*, 193 F. Supp. 3d 585, 602 (E.D. Va. 2016) (citing *United States v. Johnson*, 599 F.3d 339, 343 (4th Cir.2010)) (internal citations and quotations

omitted) (emphasis added). In this case, for the reasons discussed, there were no facts proffered to support the FBI's bare conclusions.

III. MR. SANDERS IS ENTITLED TO A *FRANKS* HEARING AS AGENT FORD KNEW OR SHOULD HAVE KNOWN THAT THE SEARCH WARRANT AFFIDAVIT INACCURATELY CONVEYED THE FLA'S TIP AND THAT THE WARRANT CONNECTED THE SANDERS FAMILY'S IP ADDRESS TO [redacted] EVEN WHEN THERE WAS NO EVIDENCE TO SUPPORT THAT LINK.

A. To the extent the Court continues to rely on a version of the FLA's tip that connotes the accessing of illegal content, as opposed to merely accessing the website itself, Mr. Sanders is entitled to a *Franks* hearing regarding the false and misleading nature of paragraph 23.

For the reasons stated above, it is now beyond any reasonable dispute that the FLA's tip meant that the Internet user merely visited the website. In suggesting more to the Magistrate, however, Paragraph 23 of the Affidavit materially overstated the FBI's contemporaneous understanding of the FLA's evidence. Thus, to the extent the Court continues to rely on the allegation that the Internet user accessed illegal content in determining whether there was probable cause, Mr. Sanders is plainly entitled to a *Franks* hearing to disprove that claim.

B. If the target website is [redacted] a fact not reflected in any document produced by the government notwithstanding Mr. Sanders's motions to compel—then Agent Ford's statement that the website had "active users" was false.

While the Affidavit supporting the search warrant itself expressly refers to an August 2019 document where the FLA "named and described the Target Website" that Mr. Sanders's IP address was supposedly used to visit, the government has refused to produce that document. In fact, the government has never produced any [redacted] document linking Mr. Sanders's IP address to [redacted] The only [redacted] document the government has produced mentioning [redacted] is the October 25, 2019 Intelligence Report (Dkt. 253-3), which has a different operation name. The government concedes, however, that the Intelligence Report has nothing to do with Mr. Sanders.

In addition, the Affidavit submitted in support of the search warrant indicates that the target website was *not* [redacted] either the website was seized in June 2019 and no longer had active users, or it was not seized and was still operating in February 2020, when Agent Ford submitted his affidavit. Because the Affidavit is indisputably false on this point, Mr. Sanders has made "a substantial preliminary showing that a false statement knowingly and intentionally, or with reckless disregard for the truth, was included by the affiant in the warrant affidavit." *Franks v. Delaware,* 438 U.S. 154, 155–56 (1978); *United States v. Clenney*, 631 F.3d 658, 663 (4th Cir. 2011). Mr. Sanders is therefore entitled to a *Franks* hearing.

CONCLUSION

The search warrant was not supported by probable cause. Furthermore, because the Affidavit was "so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable," *Leon*, 468 U.S. at 932, the good faith exception does not apply. As a result, all evidence derived from the illegal search of the Sanders's family home must be suppressed. In the alternative, because the Affidavit also includes material false statements, the Court should order a hearing under *Franks v. Delaware*.

Respectfully submitted,

/s/
Jonathan Jeffress (#42884)
Jade Chong-Smith (admitted *pro hac vice*)
KaiserDillon PLLC
1099 Fourteenth St., N.W.; 8th Floor—West
Washington, D.C. 20005
Telephone: (202) 683-6150
Facsimile: (202) 280-1034
Email: jjeffress@kaiserdillon.com
Email: jchong-smith@kaiserdillon.com

/s/
Nina J. Ginsberg (#19472)
Zachary Deubler (#90669)
DiMuroGinsberg, P.C.
1101 King Street, Suite 610
Alexandria, VA 22314
Telephone: (703) 684-4333
Facsimile: (703) 548-3181
Email: nginsberg@dimuro.com
Email: zdeubler@dimuro.com

/s/
Mark J. Mahoney (admitted *pro hac vice*)
Harrington & Mahoney
70 Niagara Street, 3rd Floor
Buffalo, New York 14202-3407
Telephone: 716-853-3700
Facsimile: 716-853-3710
Email: mjm@harringtonmahoney.com

/s/
H. Louis Sirkin (*pro hac vice* pending)
600 Vine Street, Suite 2700
Cincinnati, OH 45202
Telephone: (513) 721-4450
Facsimile: (513) 721-0109
Email: hls@santenhughes.com

Counsel for Defendant Zackary Ellis Sanders

CERTIFICATE OF SERVICE

I hereby certify that on this 17th day of September 2021, the foregoing was served electronically on the counsel of record through the US District Court for the Eastern District of Virginia Electronic Document Filing System (ECF) and the document is available on the ECF system.

/s/ Jonathan Jeffress
Jonathan Jeffress